Draft VVSG 2007 Requirements: Cryptography and Access Control

Presentation for the
Technical Guidelines Development Committee (TGDC)

Nelson Hastings

March 29, 2005
National Institute of Standards and Technology

Overview

- Draft Cryptography Requirements
- Draft Access Control Requirements
- Other VVSG 2007 Draft Requirements
- Discussion

Draft Cryptography Requirements

- Security services supported
  - Integrity
  - Confidentiality
  - Authentication
- Consolidated general cryptography requirements in a single section
- Cryptographic voting protocols NOT covered
  - Being developed under Independent Verification (IV) requirements

Topics Covered

- Algorithms
  - Symmetric and Asymmetric
  - Hash
  - Message Authentication Codes
- Validated cryptographic modules
- Security Strength
- Key Management
  - Symmetric key management
  - Public and Private key management
- General Application

Sample Draft Requirements

- Cryptographic operations shall be performed within a FIPS 140-2 level 1 or higher validated cryptographic module.
  - Many of the cryptography requirements can be met by using a validated module
  - Leverages the well established Cryptographic Module Validation Program (CMVP)

Sample Draft Requirements

- Vendors shall provide the model key management policy under which the voting system was designed to operate and a description of the hazards when deviating from the policies in the user documentation.

Sample Draft Requirements

- The integrity and confidentiality of the communications shall be protected by cryptographic means unless either:
  - (a) the communications channel between the components is entirely within a protected physical enclosure of the voting system, or
  - (b) the integrity and confidentiality of the communications is documented not to be necessary for the reliability and security of the voting system.

Continued Development

- Refine and modify requirements
  - Comments
  - Key export by general voting system

Draft Access Control Requirements

- More specificity and broaden
  - Identify people, applications, and components with respect to their role in the voting system
  - Expand authentication techniques
    - VVSG 2005 and IEEE P1586 are password centric
    - Biometrics, cryptographic tokens, etc.
  - Use modes of operation to limit access and functionality
- Physical and hardware access controls NOT covered

Topics Covered

- Documentation
- Security Policy Template
- Identification
- Authentication
- Authorization
- Logging
- Access Control Enforcement
- Communications

Sample Draft Requirements

- The voting system shall be capable of operating in at least the following modes: pre-voting, open, suspended, and post-voting.
- The voting system shall be capable of applying different access controls for each mode.

Sample Draft Requirements

- The voting system shall be capable of identifying users, systems, applications, and processes using identity-based or role-based methods.
- The voting system shall be capable of identifying, at a minimum, the groups/roles outlined in Table 2.
  - Voter, Election Judge, Poll Worker, Central Election Official, Administrator, System

Continued Development

- Refine and modify requirements
  - Comments
  - Additional research
    - ANSI/INCITS 359-2004 standard on role based access
    - IEEE P1583 and VVSG 2005

Next Draft VVSG 2007 Requirements

- Research and develop draft requirements for:
  - System Event Logging and Auditing
  - Communications
  - Software Distribution
- Draft requirements in the June 2006 timeframe

Other Draft VVSG 2007 Requirements

- Software Installation and Update
- Setup Validation
- Physical Security
- Hardware Security
- Independent Verification (IV)
- System Integrity Management
- Threat Analysis Appendix

Discussion